

## MÁS DE 19 600 INSTALACIONES PÚBLICAS DE ZIMBRA VULNERABLES A ATAQUES DE EJECUCIÓN DE CÓDIGO: CVE-2024-45519

Una vulnerabilidad crítica en el servicio postjournal de Zimbra, identificada como CVE-2024-45519, ha dejado más de 19.600 instalaciones públicas de Zimbra expuestas a ataques de ejecución remota de código.

[Más Información](#)

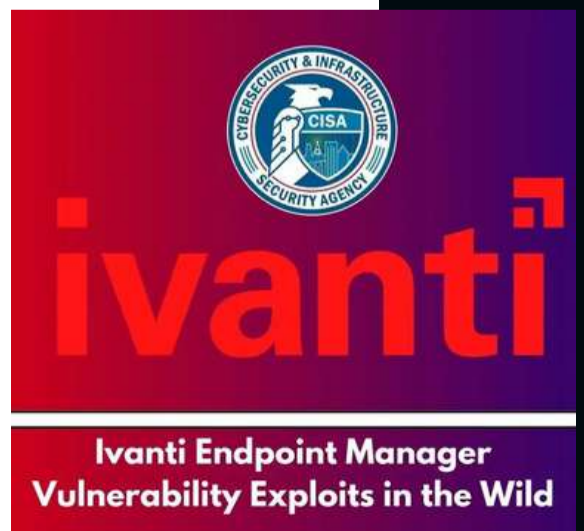
## MICROSOFT Y EL DEPARTAMENTO DE JUSTICIA DESMANTELAN CIENTOS DE SITIOS WEB UTILIZADOS POR PIRATAS INFORMÁTICOS RUSOS

Microsoft y el Departamento de Justicia de Estados Unidos (DOJ) han interrumpido las operaciones de Star Blizzard, un conocido grupo de piratas informáticos ruso.

[Más Información](#)

## LOS PIRATAS INFORMÁTICOS AHORA APROVECHAN LA VULNERABILIDAD DE IVANTI ENDPOINT MANAGER PARA LANZAR CIBERATAQUES

La Agencia de Seguridad Cibernética y de Infraestructura (CISA) ha anunciado la incorporación de una nueva vulnerabilidad a su Catálogo de Vulnerabilidades Explotadas Conocidas.

[Más Información](#)



## LA NUEVA BOTNET GORILLA LANZA MÁS DE 300.000 ATAQUES DDOS EN 100 PAÍSES

La empresa de ciberseguridad NSFOCUS, que identificó la actividad el mes pasado, dijo que la botnet "emitió más de 300.000 comandos de ataque, con una densidad de ataque impactante" entre el 4 y el 27 de septiembre de 2024.

[Más Información](#)

## INCIDENTES DE SISTEMAS

### VULNERABILIDAD DE RCE (CVE-2024-30052) QUE PERMITE A LOS ATACANTES EXPLOTAR VISUAL STUDIO A TRAVÉS DE ARCHIVOS DE VOLCADO

El investigador investigó los posibles riesgos de seguridad asociados con la depuración de archivos de volcado en Visual Studio, centrándose en las vulnerabilidades que podrían explotarse sin depender de la corrupción de la memoria o de componentes específicos del archivo PDB.

[Más Información](#)

## CVE-2024-30052 Visual Studio Exploit



### EL NUEVO MALWARE PERFCTL ATACA SERVIDORES LINUX PARA MINAR CRIPTOMONEDAS Y PIRATEAR SERVIDORES PROXY

Los servidores Linux mal configurados y vulnerables son el objetivo de una campaña en curso que distribuye un malware sigiloso denominado `perfctl` con el objetivo principal de ejecutar un software de minería de criptomonedas y proxyjacking.

[Más Información](#)



### UN FALLO CRÍTICO DEL SDK DE APACHE AVRO PERMITE LA EJECUCIÓN REMOTA DE CÓDIGO EN APLICACIONES JAVA

Se ha revelado una falla de seguridad crítica en el kit de desarrollo de software (SDK) Java de Apache Avro que, si se explota con éxito, podría permitir la ejecución de código arbitrario en instancias susceptibles.

[Más Información](#)





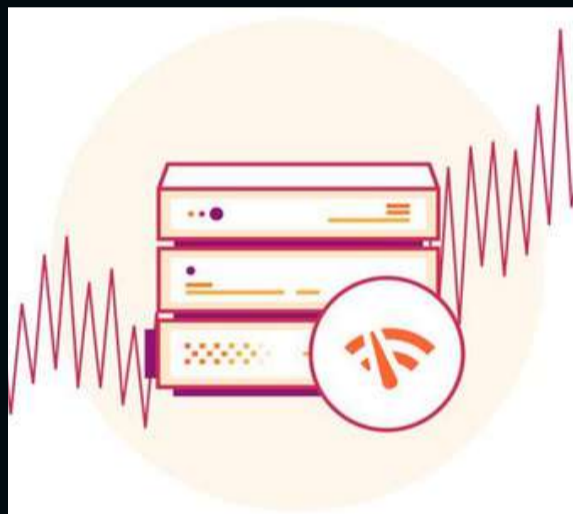
# RECOMENDACIONES

LECTURA DE SEGURIDAD

## LAS API VULNERABLES Y LOS ATAQUES DE BOTS CUESTAN A LAS EMPRESAS HASTA 186 MIL MILLONES DE DÓLARES AL AÑO

Las organizaciones pierden entre 94 y 186 mil millones de dólares al año debido a API (interfaces de programación de aplicaciones) vulnerables o inseguras y al abuso automatizado por parte de bots.

[Más Información](#)



## CLOUDFLARE FRUSTRA EL MAYOR ATAQUE DDOS DE 3,8 TBPS DE LA HISTORIA DIRIGIDO A SECTORES GLOBALES

Cloudflare ha revelado que ha mitigado un ataque de denegación de servicio distribuido (DDoS) récord que alcanzó un máximo de 3,8 terabits por segundo (Tbps) y duró 65 segundos.

[Más Información](#)

## CONOZCA EL MODELO DE RESPONSABILIDAD COMPARTIDA CON LOS NUEVOS RECURSOS DEL CIS

No puedes cumplir con tu parte del modelo de responsabilidad compartida si no haces hincapié en las configuraciones seguras. Según los servicios en la nube que uses, eres responsable de configurar diferentes cosas.

[Más Información](#)

Cloud Security  
and the Shared  
Responsibility Model  
with CIS



## CERANAKEEPER, UN NUEVO ACTOR DE AMENAZAS QUE ABUSA DE SERVICIOS COMO DROPBOX, ONEDRIVE Y GITHUB

Los investigadores de ESET observaron varias campañas dirigidas a instituciones gubernamentales en Tailandia, a partir de 2023.

[Más Información](#)

# NOTICIAS DE NUESTROS PARTNERS



## CUADRANTE MÁGICO DE GARTNER® 2024 PARA LA GESTIÓN DE ACCESO PRIVILEGIADO (PAM)

Por sexto año consecutivo, BeyondTrust ha sido reconocido como líder en el Cuadrante Mágico™ de Gartner® para la gestión de acceso privilegiado .

[Más Información](#)



Figure 1: Magic Quadrant for Privileged Access Management



Gartner

## PRESENTAMOS LA DETECCIÓN Y RESPUESTA EN MÚLTIPLES NUBES EN TIEMPO REAL IMPULSADA POR IA

Este blog anuncia la disponibilidad general del soporte de Microsoft Azure para Darktrace/CLOUD, lo que permite la detección y respuesta en la nube en tiempo real en entornos dinámicos de múltiples nubes.

[Más Información](#)



## IBM OFRECE MAYOR RENDIMIENTO Y EFICIENCIA PARA IA Y HPC CON NVIDIA ACCELERATED COMPUTING

A pesar del creciente interés en la IA generativa, solo el 39 % de las organizaciones encuestadas afirman que actualmente están implementando u operando IA generativa para la innovación y la investigación.

[Más Información](#)





# BENCHMARKING EN CIBERSEGURIDAD

Nos es muy grato informarle que, como parte de la estrategia de difusión de los servicios de Riesgo y Seguridad de Mainsoft, hemos creado una serie de benchmarkings sin costo para empresas seleccionadas.

MIDE LA SEGURIDAD DE TU ORGANIZACIÓN SIN COSTO

[HAZ CLICK](#)

EVENTOS CERCANOS DE

## NUESTROS PARTNERS

**DARKTRACE**

[Más Información](#)

 **BeyondTrust**

[Más Información](#)

 **CYLANCE**

[Más Información](#)

  
Gold Partner

[Más Información](#)

